La Cyberdéfense : un enjeu mondial, une priorité nationale

Autor(en): **Bockel, Jean-Marie**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2012)**

Heft 6

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-514712

A l'université d'été de la cyber défense 2012, l'armée française a annoncé qu'elle engageait pour cette tâche un nombre important de réservistes.

Cyber-défense

La Cyberdéfense : Un enjeu mondial, une priorité nationale

Jean-Marie Bockel

Sénateur du Haut-Rhin, ancien ministre. Auteur d'un rapport d'information sur la cyberdéfense, présenté au nom de la commission des Affaires étrangères, de la défense et des forces armées du Sénat (http// :www.senat.fr)

Attaque informatique d'envergure de Bercy à la veille de la présidence française du G8 et du G20, espionnage informatique des entreprises à l'image d'AREVA, perturbations de sites Internet comme celui du Sénat : les attaques contre les systèmes d'information se sont multipliées en France, comme partout ailleurs dans le monde, ces dernières années. Même la Présidence de la République aurait été victime récemment d'une ou de plusieurs attaque(s) informatique(s).

Ces attaques illustrent une nouvelle fois une menace encore mal connue en Europe et singulièrement en France, mais croissante : les atteintes portées à la sécurité des systèmes d'information susceptibles de mettre en cause la défense et la sécurité nationale et elles ont mis en évidence toute l'importance des moyens de se protéger de cette menace, ce que l'on désigne habituellement sous le terme de « cyberdéfense. »

Avec le développement de l'Internet, les systèmes d'information sont devenus les « centres nerveux » de nos sociétés, sans lesquels elles ne pourraient plus fonctionner. Dans ce contexte, la France est-elle suffisamment organisée et préparée pour faire face à une attaque contre les systèmes d'information ?

Il n'y a pas de « ligne Maginot » dans le cyberespace

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, il ne se passe pratiquement pas une semaine sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de gouvernements ou de grands organismes publics ou privés.

On estime qu'en France nos grandes institutions et nos entreprises sont victimes chaque jour de plusieurs millions de tentatives d'intrusions dans les systèmes d'information.

Ces attaques peuvent être menées par des pirates informatiques, des groupes d'activistes, des organisations criminelles, mais aussi par des entreprises concurrentes, voire par d'autres Etats. Les soupçons se portent souvent vers la Chine ou la Russie, même s'il est très difficile d'identifier précisément les auteurs de ces attaques.

Par ailleurs, les révélations du journaliste américain David Sanger sur l'implication des Etats-Unis dans la conception du virus STUXNET, qui a endommagé un millier de centrifugeuses d'enrichissement de l'uranium, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran, ou encore la récente découverte du virus FLAME, vingt fois plus puissant que STUXNET, laissent présager de futures « armes informatiques » aux potentialités encore largement ignorées.

On peut s'interroger sur la nature de cette menace. Peut-on véritablement parler de « cyberguerre » ? Peut-on imaginer que des conflits se joueront sur des cyberattaques, qui se substitueraient aux modes d'action militaires traditionnels ? C'est sans doute une hypothèse assez extrême. Il est acquis en revanche que l'on ne peut guère concevoir désormais de conflit militaire sans qu'il s'accompagne d'attaques sur les systèmes d'information. C'est par exemple ce qui s'est passé en Géorgie en août 2008. Toutes les armées modernes ont commencé à intégrer ce facteur. On ne peut pas éviter de telles attaques. Mais on peut en limiter les effets en renforçant les mesures de protection et en prévoyant comment gérer la crise le temps du rétablissement des systèmes.

Une menace désormais prise en compte au niveau international

Il est frappant de constater que la cyberdéfense est désormais prise en compte par nos principaux partenaires et qu'elle commence à s'affirmer au sein des instances internationales, à l'image de l'OTAN ou de l'Union eu-ropéenne.

Aux Etats-Unis, le Président Barack Obama s'est forte-ment engagé sur le sujet et a qualifié la cybersécurité de priorité stratégique. Il existe plusieurs organismes, au sein du Pentagone et du département chargé de la sécurité nationale, qui interviennent dans ce domaine, comme l'Agence de sécurité nationale (NSA) ou encore le Cybercommand, inauguré en 2010 et qui est chargé plus particulièrement de protéger les réseaux militaires américains. De 2010 à 2015,

le gouvernement américain devrait consacrer 50 milliards de dollars à la cyberdéfense et plusieurs dizaines de milliers d'agents travaillent sur ce sujet.
Au Royaume-Uni, le gouvernement a adopté en novembre 2011 une nouvelle stratégie en matière de sécurité des systèmes d'information. Le principal organisme chargé de la cybersécurité est *Government Communications Headquarters* (GCHQ). Le GCHQ compte environ 5'500 agents, dont environ 700 s'occupent des questions liées à la cyberdéfense. Malgré la forte réduction des dépenses publiques, le Premier ministre David Cameron a annoncé en 2010 un effort supplémentaire de 650 millions de livres sur les quatre prochaines années pour la cyberdéfense, soit environ 750 millions d'euros.
En Allemagne, le gouvernement fédéral a élaboré en février 2011 une stratégie en matière de cybersécurité. La coordination incombe au ministère fédéral de l'Intérieur, auquel est rattaché l'office fédéral de sécurité des systèmes d'information (BSI), situé à Bonn, qui dispose d'un budget annuel de 80 millions d'euro et de plus de 500 agents.
Les cyberattaques sont désormais une menace prise en compte dans le nouveau concept stratégique de l'Alliance atlantique, adopté lors du Sommet de Lisbonne en novembre 2010. L'OTAN s'est dotée en juin 2011 d'une politique et d'un concept en matière de cyberdéfense. Une autorité de gestion de la cyberdéfense, ainsi qu'un centre d'excellence sur la cyberdéfense ont été créés. Pour autant, l'OTAN n'est pas complètement armée face à cette menace. Ainsi, la principale unité informatique de l'Alliance n'est toujours pas opérationnelle 24 heures sur 24, 7 jours sur 7 et elle n'assure pas encore la sécurité de tous les réseaux de l'OTAN. Plus généralement, l'OTAN doit encore déterminer quelle attitude adopter pour répondre à des cyberattaques lancées contre l'un des Etats membres. Peut-on invoquer l'article 5 du traité de Washington en cas de cyberattaque? Les mesures de rétorsion doivent-elles se limiter à des moyens cybernétiques, ou bien peut-on également envisager des frappes militaires conventionnelles? Il n'y a pas encore de réponses claires à ces questions.
L'Union européenne a aussi un grand rôle à jouer, car une grande partie des règles qui régissent les réseaux de communications électroniques relèvent de sa compétence. Elle peut donc agir pour l'harmonisation de certaines dispositions techniques au niveau européen qui sont importantes du point de vue de la cyberdéfense. Toutefois, la Commission européenne et de nombreux pays européens ne semblent pas encore avoir pris la mesure des risques et des enjeux liés à la cybersécurité.

Les opérateurs d'importance vitale: notre «talon d'Achille»

Le constat que notre commission avait dressé dans son rapport il y a quatre ans était assez brutal: face à cette menace réelle et croissante, la France n'était ni bien

Au sein de l'armée israélienne, les spécialistes de la cyber défense s'engagent pour trois ans de formation et trois ans de service militaire. La qualité de la formation et les liens existants avec les entreprises et les start-ups du pays garantissent à ces soldats d'obtenir un contrat juteux à la fin de leur carrière militaire.

préparée, ni bien organisée. Il serait injuste de dire que rien n'avait été fait. Je pense au réseau gouvernemental ISIS pour l'information confidentiel défense. Néanmoins, les lacunes restaient criantes. Il paraissait donc indispensable d'accélérer la prise de conscience des autorités politiques, de clarifier les responsabilités au sein de l'Etat et de renforcer résolument les moyens techniques et humains nécessaires à une vraie politique de cyberdéfense.

Le Livre blanc sur la défense et la sécurité nationale de 2008 a identifié ce besoin et donné une réelle impulsion à cette politique. En termes d'organisation, le Livre blanc a permis à cette politique d'être clairement identifiée, avec la création, en juillet 2009, de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, qui est dirigée par Patrick Pailloux, dont les compétences sont reconnues par tous en France comme à l'étranger.

En février 2011, l'ANSSI a rendu publique la stratégie de la France en matière de cyberdéfense. Il a été également décidé de faire de l'ANSSI l'autorité nationale de défense des systèmes d'information. La France dispose, avec cette stratégie et avec l'ANSSI, d'outils importants en matière de cyberdéfense. Pour autant, beaucoup reste à faire dans ce domaine.

Ainsi, avec des effectifs de 230 personnes et un budget de l'ordre de 75 millions d'euros en 2012, les effectifs et les moyens de l'ANSSI sont encore très loin de ceux dont disposent les services similaires de l'Allemagne ou du Roy-aume-Uni, qui comptent entre 500 et 700 personnes. Pour accroître sa capacité d'intervention et de soutien, le gouvernement de François Fillon avait d'ailleurs décidé, en mai 2011, d'accélérer l'augmentation des effectifs et des moyens de l'ANSSI, afin de porter ses effectifs à 360 d'ici 2013.

De plus, si les armées et le ministère de la défense ont pris des mesures, les autres ministères, les entreprises et les opérateurs d'importance vitale (transports, énergie, santé, etc) restent différemment sensibilisés à cette menace.

Assurer la sécurité des systèmes d'information des entreprises n'est pas seulement un enjeu technique. C'est aussi un enjeu économique, puisqu'il s'agit de protéger la chaîne de valeur, notre savoir-faire technologique dans la véritable guerre économique que nous connaissons aujourd'hui, voire un enjeu politique, lorsque les intérêts de la nation sont en jeu. Or, avec l'espionnage informatique, la France, comme les autres pays occidentaux, est aujourd'hui menacée par un « pillage » systématique de son patrimoine diplomatique, culturel et économique.

Reste enfin, la question des opérateurs d'importance vitale. Quel serait aujourd'hui le moyen le plus simple de provoquer une perturbation majeure de notre pays par le biais d'une attaque informatique ? Un moyen très simple serait de s'en prendre aux systèmes de distribution d'énergie, aux transports ou aux hôpitaux. L'exemple du virus STUXNET, ou celui du ver Conficker qui a perturbé le fonctionnement de plusieurs hôpitaux en France et dans le monde, montrent que cela n'est pas une hypothèse d'école.

Certes, il ne s'agit pas de prétendre à une protection absolue. Ce serait assez illusoire. Le propre des attaques informatiques est d'exploiter des failles, de se porter là où les parades n'ont pas encore été mises en place. Mais on peut renforcer la sécurité des réseaux et des infrastructures les plus sensibles, et améliorer leur résilience.

La cyberdéfense : une priorité nationale

La protection et la défense des systèmes d'information devrait faire l'objet d'une véritable priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. Il me paraît ainsi indispensable de renforcer les effectifs et les moyens de l'ANSSI au moyen d'un plan pluriannuel, afin de les porter progressivement à la hauteur de ceux dont disposent nos principaux partenaires européens. Cette augmentation, de l'ordre de quelques 80 agents par an, devrait au demeurant rester modeste.

Il me semble aussi que beaucoup reste à faire pour sensibiliser les administrations, le monde de l'entreprise, notamment les PME, et les opérateurs d'importance vitale. L'ANSSI s'efforce d'inciter les entreprises à respecter des règles élémentaires de sécurité, règles que son directeur, M. Patrick Pailloux, assimile à des règles d'hygiène élémentaires, mais qui sont souvent considérées comme autant de contraintes par les utilisateurs. Faut-il aller plus loin et passer par la loi pour fixer un certain nombre de règles ou de principes ? Après avoir beaucoup consulté, je crois qu'il est nécessaire de prévoir une obligation de déclaration en cas d'attaques informatiques qui s'appliquerait aux entreprises et aux opérateurs des infrastructures vitales, afin que l'Etat puisse être réellement informé de telles attaques.

Je pense aussi que l'Etat a un rôle important à jouer pour soutenir le tissu industriel, et notamment les PME, qui développent en France des produits ou des services de sécurité informatique, pour ne pas dépendre uniquement de produits américains ou asiatiques. Je plaide ainsi dans mon rapport pour une politique industrielle volontariste, à l'échelle nationale et européenne, pour faire émerger de véritables « champions » nationaux ou européens.

A cet égard, j'insiste dans mon rapport sur la question des « routeurs de cœur de réseaux. » Ces « routeurs » sont de grands équipements informatiques utilisés par les opérateurs de télécommunications pour gérer les flux de communications (comme les messages électroniques ou les conversations téléphoniques) qui transitent par l'Internet. Ils représentent des équipements hautement sensibles car ils ont la capacité d'intercepter, d'analyser, d'exfiltrer, de modifier ou de détruire toutes les informations qui passent par eux.

Actuellement, le marché des routeurs est dominé par des entreprises américaines, comme Cisco, mais, depuis quelques années, des entreprises chinoises, à l'image de Huawei et ZTE, font preuve d'une forte volonté de pénétration sur le marché mondial et en Europe.

Or, cette stratégie soulève de fortes préoccupations, en raison des liens de ces entreprises avec le gouvernement chinois et des soupçons d'espionnage informatique qui pèsent sur la Chine. Ainsi, les autorités américaines, comme d'ailleurs les autorités australiennes, ont refusé l'utilisation de « routeurs » chinois sur leur territoire pour des raisons liées à la sécurité nationale. En Europe, une telle interdiction semble plus délicate mais la Commission européenne s'apprêterait à lancer une procédure d'infraction à l'encontre de ces entreprises, soupçonnées de concurrence déloyale.

Pour ma part, je considère qu'il est indispensable que l'Union européenne, à l'image des Etats-Unis ou de l'Australie, interdise l'utilisation des « routeurs » ou autres équipements informatiques sensibles d'origine chinoise sur son territoire. Il s'agit là d'un véritable enjeu de sécurité nationale.
Se pose également la question des ressources humaines. Il existe aujourd'hui peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à en recruter. Nous devrions mettre l'accent sur la formation et développer les liens avec les universités et les centres de recherche. Pourquoi ne pas renforcer aussi les liens avec la « communauté de hackers », dont la plupart sont désireux de mettre leurs compétences et leurs talents au service de leur pays ?
Il paraît également nécessaire de renforcer la sensibilisation des utilisateurs. De même qu'il existe un plan de prévention en matière de sécurité routière, pourquoi ne pas imaginer une campagne de communication en matière de sécurité informatique ?
Face à une menace qui s'affranchit des frontières, la coopération internationale sera déterminante. Elle existe d'ores et déjà entre les cellules gouvernementales spécialisées ou de manière bilatérale, notamment avec nos partenaires britanniques ou allemands. Elle arrive à l'ordre du jour d'enceintes internationales comme l'OTAN ou l'Union européenne, qui pourrait s'impliquer plus activement, par exemple pour imposer un certain nombre de normes de sécurité aux opérateurs de réseaux.
Pour autant, si la coopération internationale est indispensable, notamment avec nos partenaires britanniques et allemands, il ne faut pas se faire trop d'illusions. La cyberdéfense est une question qui touche à la souveraineté nationale et il n'existe pas réellement d'alliés dans le cyberespace.
Enfin, je pense qu'il faut nous poser la question délicate des capacités offensives. Il existe sur ce sujet en France un véritable « tabou ». A l'inverse, d'autres pays, comme les Etats-Unis ou le Japon, n'hésitent pas à affirmer qu'ils répondront à une attaque informatique. Pour ma part, je pense qu'on ne peut pas se défendre si l'on ne connaît pas les modes d'attaque.
La lutte informatique offensive est prévue par le Livre blanc de 2008 et la loi de programmation militaire. Mais toutes ses implications ne sont pas aujourd'hui clarifiées. Comment savoir si une attaque se prépare ou est en cours ? Comment établir l'identité des agresseurs ou la responsabilité d'un Etat ? Quelle doctrine d'emploi adopter ? Il faudra que nos experts trouvent des réponses à ces questions. Dans mon rapport, je m'interroge donc sur l'opportunité de définir une doctrine publique sur les capacités offensives, qui pourrait être reprise par le nouveau Livre blanc sur la défense et la sécurité nationale.
En définitive, compte tenu de la place croissante des systèmes d'information et d'Internet dans le fonctionnement de nos sociétés, je suis convaincu que notre défense et notre sécurité se joueront aussi sur les réseaux informatiques dans les années futures.

J.M. B.

Message du CdA

Une chance pour la milice

Chères lectrices, chers lecteurs,
« Une chance pour la milice » et la Société des officiers du canton de Lucerne ont organisé récemment une rencontre à Lucerne, en même temps que le séminaire pour jeunes officiers de la SSO. Les organisateurs s'étaient posé la question de savoir si la « génération Facebook » et l'armée de milice avaient encore des points communs. La réponse à cette question a déjà été donnée par le fait que la SO Lucerne, sous la conduite de son jeune président, a organisé cette rencontre à la perfection et que plus d'une trentaine de jeunes officiers y ont participé. Si l'on considère encore les discussions menées lors de cette rencontre, on constate que nos jeunes, par leur point de vue différent et par leur engagement important, apportent aussi leur contribution à notre société. Les jeunes adultes ont aujourd'hui tellement de possibilités de formation continue qu'ils n'ont que l'embarras du choix. Si la volonté de l'Etat est d'engager des jeunes gens bien formés au profit de la sécurité du pays, on peut dire que l'obligation de servir et le système de milice sont des éléments importants et pertinents dans ce contexte.
Quand, lors de la même manifestation, le professeur de sociologie Bergman, outre ses explications sur les conséquences des médias sociaux, parle accessoirement d'un risque de guerre fortement accru en raison des tensions croissantes dans le monde tant sur le plan social qu'économique, ce sont forcément des propos qui éveillent l'attention.
La fin de l'année est proche. Au moment où vous tenez cette édition entre les mains, la période de l'avent commence. Ce sont des jours propices au recueillement. Nous avons généralement la chance de pouvoir les passer en paix et en famille, ce qui n'est pas le cas dans de nombreuses parties du monde. N'oublions pas que ce sont nos concitoyens qui, par leur engagement, contribuent à notre sécurité.
Je vous souhaite une période de Noël pleine de sérénité et je remercie tous les militaires en service et leurs proches, sans oublier les employeurs, de leur engagement au profit de la sécurité de notre pays.

Commandant de Corps André Blattmann, Chef de l'Armée

News

Nouvelle munition RUAG

Afin d'améliorer sensiblement les performances des armes chambrées en .223 Remington (5,56x45 mm standard OTAN), fusils d'assaut et mitrailleuses légères, le
munitionnaire suisse RUAG a développé et réalisé une toute nouvelle munition AP (armour-piercing) à très haut pouvoir de perforation.
Baptisée 5,56 x 45 LF+HC Horizon, cette nouvelle munition est en mesure de percer 7 mm d'acier HB350 à 300 rn ou 10 mm d'acier mou à 600 m. Cet étonnant résultat a pu être obtenu en utilisant une balle entièrement chemisée en acier, dont le poids représente ni plus ni moins les deux tiers de la masse totale du projectile. La munition LF+HC Horizon utilise une poudre non toxique, qui assure un maximum de stabilité, même en condition de températures extrêmes (de -54oC à + 52oC), tout en réduisant aussi bien la flamme de départ que l'usure du canon et l'accumulation des résidus de poudre. Comme toute la gamme de munitions RUAG, la nouvelle AP suisse est fabriquée avec des composants de la meilleure qualité et elle est soumise à des contrôles de fabrication rigoureux afin de garantir une parfaite fiabilité.